L Number	Hits	Search Text	DB	Time stamp
1	48	("5963644" "4888802" "5434920" "5455861" "5594798" "5974142" "6253193" "6363488" "6389402" "6427140" "6070245" "4369332" "5371797" "5960086" "5978918" "5579394" "5920627" "5392357" "5222136" "5416842" "5588060" "5633933" "6363154" "4860352" "5243653" "6092200" "5392355" "5428686" "6226751" "6226751" "5365590" "6061796" "6061796" "6158011" "5608733" "6205142" "5272754" "5307410" "6442696" "5479514" "5214698" "5615264" "5764762" "6246771" "6483919" "6021203" "5237611" "5414773" "5442708" "5444782").pn.	USPAT	2003/11/06 12:20
2	1	4635223.pn.	USPAT	2003/11/06 11:28
3	15106	4635223.pn. fail adj safe	USPAT	2003/11/06 11:27
4	1	4635223.pn. and (fail adj safe)	USPAT	2003/11/06 11:28

5	9	(("5963644" "4888802" "5434920" "5455861" "5594798" "5974142" "6253193" "6363488" "6389402" "6427140" "6070245" "4369332" "5371797" "5960086" "5978918" "5579394" "5920627" "5392357" "5222136" "5416842" "5588060" "5633933" "6363154" "4860352" "5243653" "6092200" "5392355" "5428686" "6226751" "6226751" "5365590" "6061796" "6061796" "6158011" "5608733" "6205142" "5272754" "5307410" "6442696" "5479514" "5214698" "5615264" "5764762" "6246771" "6483919" "6021203" "5237611" "5414773" "5442708" "5444782").pn.) and verif$5 with key$1	USPAT	2003/11/06 12:24
6	30	"back up" with key$1 and "fail safe"	USPAT	2003/11/06 12:33
7	0	"back up" with key$1 and "fail safe" and (prevent with regenerat$4 with key$1)	USPAT	2003/11/06 12:28
8	0	"back up" with key$1 and "fail safe" and suspend and (regenerat$5 with key$1)	USPAT	2003/11/06 12:28
9	13	"back up" with key$1 and "fail safe" and suspend	USPAT	2003/11/06 12:31
10	0	"back up" with key$1 with generat$4 with suspend	USPAT	2003/11/06 12:34
11	1	"back up" with key$1 with generat$4 with prevent	USPAT	2003/11/06 12:34
-	143	713/150.ccls.	USPAT	2003/11/04 16:39
-	0	380/49.ccls.	USPAT	2003/11/04 18:18
-	4	5594798.pn.,5579394.pn.,5077791.pn.,4815128.pn.	USPAT	2003/11/04 19:33
-	189	713/156.ccls.	USPAT	2003/11/04 18:26
-	5	713/156.ccls. and (vpn or "virtual private network")	USPAT	2003/11/04 18:52
-	165	713/153.ccls.	USPAT	2003/11/04 18:31
-	14	713/153.ccls. and vpn	USPAT	2003/11/04 18:41

US-PAT-NO: 4091423

DOCUMENT-IDENTIFIER: US 4091423 A

TITLE: Synchronous digital data scrambling system

---------- KWIC ---------

Detailed Description Text - DETX (9):
The synchronizer generates a signal to the controller 36 which monitors the various control signals coming from the facsimile machine and sequences all of the operations within the facsimile scrambler. The controller 36 contains a fail-safe alarm circuit used to continuously monitor the output of the enciphered bit stream to detect indications of key generator failure while in the private transmitting mode. In addition, the overall system has been designed in such a way that no single failure in the private mode can cause inadvertent transmission of clear text.

Detailed Description Text - DETX (13):
Operation of the system shown in FIG. 2 is fully automatic, thereby allowing completely unattended reception of both clear and private scramble messages intermixed with one another. Normal facsimile transmission in the private mode requires no special action on the part of the operator. Usually, the operator will be unaware that the scrambler is in use. If the operator chooses to send a picture or document in clear mode, the operator must make a special effort and depress the clear push button 38. The clear push button 38 must be depressed until the clear indicator comes on at the beginning of the

transmission, afterwhich the clear indicator light will show that the machine
is in the clear mode. The system has a special alarm circuit which monitors
the output of the key generator 40 for a failure which would compromise the
transmission. In addition, if there is a power failure or if other critical
components in the scrambler fail during a transmission, the system goes into an
alarm state and opens the transmit video path.

Detailed Description Text - DETX (123):
The clear facsimile signal to be scrambled by the present device is normally
quantized into black or white information, enciphered and transmitted via the
built-in facsimile machine modem. In applications wherein higher security,
resulution and a lower error rate are required, an external modem may be
utilized. Operation of the present device is fully automatic, thereby allowing
completely unattended reception of both clear and private scramble messages
intermixed. Normal facsimile transmission in the private mode requires no
special action on the part of the operator. The present system is designed in
such a manner that no single failure in the scramble mode can cause inadvertent
transmission of clear text. A fail-safe circuit is utilized to continuously
monitor the output scramble bit stream for key generator failure while in the
transmit scramble mode.

US-PAT-NO: 6209091

DOCUMENT-IDENTIFIER: US 6209091 B1

TITLE: Multi-step digital signature method and system

---------- KWIC ---------

Brief Summary Text - BSTX (4):

Thus far, the need for security of a CA's private signature key has been addressed by providing a "certificate signing unit" (CSU), which is a tamper-proof secure module satisfying standards set forth in Federal Information Processing Standard (FIPS) PUB 140-1, level 3 or 4 as issued by the U.S. Dept. of Commerce, National Institute of Standards and Technology (NIST). Such a CSU generates its public/private signature key pair internally, "confines" the private signature key securely and permanently inside an area of the device that cannot be read externally, and outputs only the corresponding public key, which will be used to verify its signatures. One CSU available from Bolt, Baranek, and Newman of Boston, Mass. (BBN) is configured to allow a back-up version of its private signature key to be created using a "K-of-N threshold" scheme, in which the private key is split into N shares and placed on small plastic data-keys, each of which contains a memory chip. The data-keys are a patented product of Datakey, Inc. of Burnsville, Minn. Then, should the CSU device be destroyed, a quorum of at least K data-keys can reconstruct the private key.

Brief Summary Text - BSTX (14):

If, during the initial generation of operational shares, a whole signature key is generated, the whole signature key is destroyed after shares are distributed. Because the risk of loss from the theft or compromise of any one device is now greatly reduced, the information content of each signing device can be now duplicated (e.g., for remote backup or for a plug-in replacement or "hot" standby) so that if any device fails, it can be replaced (or reconstituted) and service can resume quickly. The consequence of subversion of any individual signing device is lowered, because the signing operation cannot be completed with a single device.

Detailed Description Text - DETX (158):

The risk (consequences) of theft or destruction of signing devices has been reduced by virtue of the multi-step signing process and the fact that no single signing device is capable of forging a signature or divulging information sufficient to forge a signature. The information content of a signing device, including the SWA key share, can therefore be transferred to another device, e.g., when upgrading signing device hardware or for back-up purposes.

Detailed Description Text - DETX (185):

As an alternate back-up method, up the decryption key shares can be escrowed off-line with an independent trust institution as described in copending U.S. patent application Ser. No. 08/181,859 now abandoned and Ser. No. 08/277,438 now abandoned.